REMARKS

I. INTRODUCTION

Claims 1, 3-6, 8-12, 14-16 and 18 have been amended to more distinctly claim and particularly point out that which Applicants regard as the subject matter of the invention. Claims 1-18 remain pending in the present application. No new matter has been added. In view of the above amendments and the following remarks, it is respectfully submitted that all of the presently pending claims are allowable.

II. THE 35 U.S.C. § 102(b) REJECTIONS SHOULD BE WITHDRAWN

Claims 1-5 have been rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,712,912 to Tomko et al. ("the Tomko reference").

The Tomko reference describes a PIN generating apparatus which includes an encrypting device and a decrypting device. (See the Tomko reference, col. 3, lines 43-45). An individual's fingerprint is read from a biometric input device 10, converted to a biometric information signal and sent to a processor 24. (See the Tomko reference, col. 3, line 66 - col. 4, line 5). A random character generator outputs a digital PIN which is encrypted by the processor 24 using the biometric information signal. (See the Tomko reference, col. 4, lines 6-9). The encrypted PIN is stored in a storage means 30, such as a credit card. (See the Tomko reference, col. 4, lines 9-11). When decrypting the PIN, a processor 24 reads the encrypted PIN from the storage means 30 and another fingerprint from the biometric input device 10. (See the Tomko reference, col. 4, lines 18-28). The PIN is only decrypted if the fingerprint is the same as the one used to encrypt the PIN. (See the Tomko reference, col. 4, lines 25-27). Thus, the biometric information (i.e., fingerprint data) is not stored by the processor 24.

Claim 1 of the present invention recites a semiconductor device for securely controlling access to cryptographic processing of data which comprises "a semiconductor package" and "a cryptographic processor disposed in the semiconductor package, *the processor including a biometric data capture device operative to acquire biometric data associated with a predetermined biometric characteristic of a user and store the biometric data as a biometric key*, and an encryption/decryption circuit operative to perform encryption or decryption on input data utilizing said biometric key." According to the specification, "the sensor 11 registers the actual biometric data, and processes and stores in [sic] the module 10." (See Specification, page 15). In this manner, the present invention can "receive encrypted data input using the biometric key as an encryption parameter," and "decrypt the data input using the stored biometric key." (See Specification, page 17). Thus, the claim and the specification make it clear that the biometric data is stored by the cryptographic processor.

In contrast, the Tomko reference describes storage of an encrypted PIN, not biometric data (e.g., fingerprint). Furthermore, the PIN is stored on an external device such as a credit card and not within the cryptographic processor. There is no teaching or suggestion in the Tomko reference that biometric data should be stored within the cryptographic processor. Therefore, it is respectfully submitted that the Tomko reference does not disclose or suggest "the processor including a biometric data capture device operative to acquire biometric data associated with a predetermined biometric characteristic of a user and store the biometric data as a biometric key," as recited in claim 1.

It is respectfully submitted that claim 1 is not anticipated by the Tomko reference for the reasons discussed above and that this rejection should be withdrawn. Because claims 2-5 depend from and, therefore, include all of the limitations of claim 1, it is respectfully submitted that these claims are also allowable.

III. THE 35 U.S.C. § 103(a) REJECTIONS SHOULD BE WITHDRAWN

Claims 6-10 have been rejected under 35 U.S.C. §103(a) as being unpatentable over the Tomko reference in view of U.S. Patent No. 6,085,976 to Sehr ("the Sehr reference").

Independent claim 6 recites "the processor including a biometric data capture device to capture biometric data associated with predetermined biometric characteristic of a user and store the biometric data as a biometric key." This limitation is similar to the recitation described above with reference to claim 1. Thus, for the same reasons as described above, the Tomko reference neither teaches nor suggests this recitation of claim 6. The Sehr reference fails to cure this deficiency of the Tomko reference. Therefore, it is respectfully submitted that neither the Tomko reference nor the Sehr reference, either alone or in combination, teaches or suggests "the processor including a biometric data capture device to capture biometric data associated with predetermined biometric characteristic of a user and store the biometric data as a biometric key," as recited in claim 6. Thus, claim 6 and claims 7-10, which depend therefrom, are allowable.

Claims 11-18 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over the Tomko reference in view of U.S. Patent No. 6,484,260 to Scott ("the Scott reference").

Independent claim 11 recites "a stored biometric key in said cryptographic processor." This limitation is similar to the recitation described above with reference to claim 1. Thus, for the same reasons as described above, the Tomko reference neither teaches nor suggests this recitation of claim 6. The Scott reference fails to cure this deficiency of the Tomko reference. Therefore, it is respectfully submitted that neither the Tomko reference nor the Scott reference, either alone or in combination, teaches or suggests "a stored biometric key in said cryptographic processor," as recited in claim 11. Thus, claim 11 and claims 12-18, which depend therefrom, are allowable.

IV. THE 35 U.S.C. § 112 REJECTIONS SHOULD BE WITHDRAWN

Claim 13 has been rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. The Examiner states that "[i]t is unclear as to how biometric data is related to encrypted biometric key." (See Office Action, 9/21/04, ¶ 5). Claim 13 recites, "the stored biometric key is encrypted biometric data from an authorized user of the network." It is respectfully submitted that this claim language is clearly described in the specification on page 16 and with regard to Figure 2. Specifically, Applicants state, "the biometric data is then encrypted, using a defined algorithm and key." (See Specification, page 16). The language is clear: the biometric key is encrypted biometric data. Therefore, Applicants respectfully request that the Examiner withdraw the rejection of claim 13 under 35 U.S.C. § 112.

V. CONCLUSION

In light of the foregoing, the applicants respectfully submit that all of the pending claims are in condition for allowance. All issues raised by the Examiner have been addressed, an early and favorable action on the merits is earnestly solicited.

Respectfully submitted,

Dated: December 21, 2004

By: _____
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, NY 10038
Tel: (212) 619-6000
Fax: (212) 619-0276